INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

The Cybercrime situation in Spain

DISSEMINATION LEVEL PUBLIC

PARTNER

GUARDIA CIVIL

AUTHOR

GUARDIA CIVIL

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

1. The Cybercrime situation in Spain[1]

2021 was the year in which most critical incidents were handled in Spain. In addition, incidents have generally shown greater sophistication, especially through zero-day remote code execution vulnerabilities, but also through supply chain compromise, as was the trend in 2020.

The use of COVID-19 as a hook in 2021 for attacks against ICT systems has decreased compared to the previous year. In this regard, it is worth recalling that during the first part of the pandemic, the use of the COVID-19 theme was mostly used in phishing campaigns by cybercriminals with a clear economic purpose. It was not until mid-2020 and during 2021 that its use was also observed, among other more targeted themes, in Advanced Persistent Threat (APT) groups related to cyber-espionage between states, whose objectives also included finding out about progress in the development of new vaccines against the disease.

As we have seen since the first quarter of 2021, the term vulnerability has been a constant throughout that year. In the wake of the exposure of remote access services, attackers have focused their efforts on gaining entry into organisations through the opportunities that teleworking has provided, including for them. Not only has it been a record year in terms of the number of vulnerabilities, but they have also been among the most critical. In the period from 2017 to 2021, there was an increase in cybercrime. Thus, we can see that, in 2021, a total of 305,477 incidents have been known, which is 6.1% more than the previous year.[2]

2. Cyber-dependent crime

2.1 Malware

The growing trend of ransomware attacks that was occurring at the end of 2020 has continued during 2021, with ransomware being the type of attack that has increased the most during the year.

Ransomware groups have started to use different extortion techniques to force payment from their victims, either by threatening to leak stolen information or by phoning the organisation's headquarters directly. Added to this is the monetisation on Dark Web forums of the exfiltrated, in 2021, a total of 109,126 cybersecurity incidents against private companies were managed in Spain.[3]

With regard to the types of malwares with the greatest relevance and effects in 2021, the following are worth mentioning:

>> **Emotet:** It works as a "downloader" allowing the download and execution of other harmful codes, as well as monitoring network traffic, obtaining any information contained in the victim's browsers, from user credentials to banking information. The most common Emotet campaigns during 2021 involved sending phishing emails with malicious attachments containing macros that functioned as malware downloaders. Most of the attachments were identified as Microsoft Office files, although other file formats such as ZIP and PDF were observed.

>> **Mekotio:** Also known as BestaFera, it represents a serious threat to all those users who make use of online banking services or cryptocurrencies, specifically Bitcoins, as it is a banking Trojan that affects all versions of the Windows operating system, from Windows XP to Windows 10. It works as a downloader, allowing the download and execution of other malicious code, as well as monitoring network traffic, obtaining any information contained in the victim's browsers. The most common Mekotio campaigns during 2021 involved sending phishing emails with malicious attachments containing macros that functioned as malware downloaders.

>> **Flubot:** Trojan-like malware for Android devices. The most common campaigns involved sending fraudulent SMS messages informing of the receipt of a package impersonating different logistics companies, such as FedEx, DHL or Correos. These messages invite the recipient to install an application on their mobile device with the incentive that they can find out the whereabouts of the package. Once the user installs the application on their device, it begins to track the identifiers of all applications that are launched, with the ability to inject overlay pages upon detecting a login to one of the targeted applications, so that the user trusts that they are entering credentials on the original website when, in reality, they are sending them to the command-and-control server controlled by the operators of the malicious code.

>> **Anatsa:** Trojan-type malware for Android devices that has been analysed, in parallel, by different organisations assigning it different names such as: Anatsa, TeaBot or Toddler. As in Flubot, once the user installs the application on their device, it starts to track the identifiers of all launched applications, with the ability to inject overlay pages when it detects a login to one of the target applications, so that the user trusts that they are entering credentials on the original website when, in reality, they are sending them to the command-and-control server controlled by the operators of the malicious code.

>> **Hive:** ransomware-type malware that implements information encryption functions on an infected computer, making it impossible to recover data easily.

On the other hand, with regard to incidents related to fraud, it should be noted that, during 2021, campaigns to impersonate customers or suppliers continued to proliferate, via telephone and e-mail, with a total of 31,529 incidents in all areas of the private sector.[4]

In terms of the main incidents, the following can be highlighted:

1. **Microsoft servers:** The attack on Microsoft's mail servers was first recognised in January. This hack alerted thousands of companies and affected more than 250,000 servers worldwide. Speculation as to who was responsible for the hack was in the air for several months, but last July the United States, the European Union and several NATO allies roundly accused China of being behind the attack.

2. **The Facebook data leak:** In March 2021, the data of a total of 533 million users, including phone numbers, full names, locations and dates of birth, were shared and exposed within Surface Web, findable with a normal search engine. In Spain alone, 11 million accounts were affected by this security breach, according to an analysis conducted by Business Insider by cross-checking information on websites and Telegram.

3. **SEPE:** Also in March, the SEPE's IT service was infected with ransomware that had the capacity to leak files and block computers. The attack paralysed more than 700 offices of the Public State Employment Service of Spain, paralysing 200,000 appointments and endangering the unemployment benefit payment system because state employees were unable to use their computers.

4. **Kaseya:** During the first weekend of July, more than 350 organisations worldwide suffered a ransomware attack on their computer systems. According to ESET, one of them was a Spanish company. The cyberattack was created by the notorious REvil group, and used an update from IT services software company Kaseya to leak the malware. Revil's cybercriminals publicised that they had infected more than one million devices and demanded around 62 million EUR in ransom.

5. **Attack on the Ministry of Labour and Economy:** In June, just three months after the attack on the SEPE, Spain was once again on the ropes, exposing its cybersecurity systems. A total of 5,500 civil servants were unable to work for more than 15 days due to a lack of their own resources and the difficulty of resolving the problem. On this occasion, the ministry turned to Fujitsu Technology Solutions S.A., awarding them a contract with an estimated value of 145,893.33 EUR. The most alarming thing is that, according to the National Cryptologic Centre, only six websites of the General State Administration currently have a National Security Scheme Conformity Certification.

6. **Attack on MediaMarkt**: Coinciding with the preparations for Black Friday, the German multinational suffered a cyber-attack at the beginning of November that affected the company's shops in Holland, Germany, Belgium and Spain. According to an internal email that has been leaked, this attack affected more than 30,000 Windows servers - for the moment - and the ransom demand is estimated to exceed 213 million EUR.

7. **Man in the middle' at Seville City Hall:** Like many others, the Seville City Council was also targeted by hackers. Using the Man in the middle tactic, they intercepted the council's email communications with a supplier, impersonated the latter and managed to modify the bank account for the payment of a service contract. In total, they misappropriated almost one million EUR.

8. **Continuing with cyberattacks against public institutions:** another of the most notorious in 2021 were those directed against city councils in different Spanish cities. The cybercriminals left the systems and websites of cities such as Fuenlabrada, Oviedo and Vinarós without connection. Other organisations affected by this type of crime were the Court of Auditors and the National Security Council (CNS). The criminals managed to encrypt part of the systems and introduce the Zeppelin ransomware, but in this case the data were properly protected and their confidentiality could be preserved.

9. **Phone House:** On 11 April 2021, the Phone House website suffered a cyber-attack. Again, a ransomware attack, with which they were able to access part of the customer database. Although the company reported that, in this case, customers' personal data had not been breached, shortly afterwards it came to light that a total of 100GB of personal data had been stolen. Moreover, according to media reports, the fraudsters demanded a ransom to keep the data from being released: "We have 10 databases containing private information (full name, date of birth, email, telephone, address, nationality...) of more than 3 million customers and employees. If you don't pay, all this information will be published on our public blog and darknet forums and sent to all your partners and competitors".

10. **Glovo, the Spanish digital home shopping and delivery company:** Glovo shared that on 29 April 2021 it had discovered unauthorised access to its systems. Forbes magazine reported that customer and delivery account data had been offered for sale on the Internet by the hacker himself. No banking or particularly sensitive data were breached in this attack, but it emerged that the affected data were not encrypted or properly protected.[5]

2.2. Hacktivism

In Spain, there is no hacktivist network that originated in the country, beyond minimal propaganda activity on social networks by identities that use hacktivist iconography. The only exception in this scenario of a lack of hacktivism with Spanish roots is the identity known as 'La 9a Compañía' or 'La9deAnon' which, nevertheless, has been carrying out cyber-attacks that have been declining towards occasionality since 2018.

This absence of a properly Spanish hacktivism does not imply that Spain's cyberspace is free of cyberattacks carried out by identities whose activities could be framed, albeit partially, in the orbit of hacktivism. On the contrary, Spain falls within the commonality of countries on any continent, in the sense that websites with a domain and/or IP address residing in its cyberspace are attacked through penetration and defacement actions, carried out by attackers from various geographic origins, who often exploit common vulnerabilities in outdated software to execute serial or mass defacements on websites in several countries. This type of hacktivism of opportunity, increasingly intersecting with practices in the initial sequence of cyberthreats for propagation, has been used by a number of different actors.

Harmful code hacktivism was common in Spain in 2021, with monthly and geographical statistics varying in each case depending on the attackers' ability to exploit software vulnerabilities wherever they can find them.

In 2021, the latent hacktivist narrative frameworks of #OpSpain or #OpCatalunya, both have been devoid of cyber offensive activity, limited to some sporadic mentions of these tags in messages on social networks, of an individual nature and without a pattern of collectivisation, and also devoid of explicit threatening semantics.

During 2021, the generic profile of hacktivism in Spain was as follows:

>> Practical non-existence of indigenous hacktivist identities, while websites in Spain form part of those commonly attacked in any country by identities operating on the basis of opportunity criteria based on the exploitation of common software vulnerabilities.

>> A couple of hacktivist identities active in Spain that can be hypothesised as originating in the country: 'La 9a Compañía', a cyberthreat focused on technique and method, i.e. equipped with sufficient technical computer skills to produce cyberattacks by penetrating web servers exposed to software vulnerabilities, using tools at their convenience; and 'jibar0', whose hacktivist background shows low to moderate technical skills, corresponding to a tool-centric cyberthreat, i.e. he can use some basic software vulnerability exploitation tools, but does not have sufficient computer skills and knowledge to develop cyberattack techniques based on the manual generation or manipulation of software code, relying, as any user would, on third-party tools, usually free software.

>> The absence or inactivity of militant narrative frameworks that promote hacktivism in Spain, as well as the lack of any discourse with hacktivist intentions.

>> With the exception of some occasional attempts that have so far failed to make an impact, the breakdown of any organised hacktivist propaganda base that could encourage the revitalisation of a hacktivist fabric that has been exhausted since the first third of the 2010s.[6]

During 2021, the trend continued for websites with IP addresses or domain names based in Spain to be compromised through defacement, as part of cyber-attack actions carried out by identities acting from outside Spain on websites anywhere in the world, which have in common exposing some kind of vulnerability in the installed software.

Similarly, a pattern of exploiting hacktivist attacks to deface websites for the injection of content to poison search engine results (a practice known as SEO poisoning, or Search Engine Optimisation) was consolidating in 2021, of scripts redirecting traffic to websites distributing malicious content, or of insertion or redirection to content simulating e-commerce environments which, in reality, are phishing traps for the theft of personal identification and payment data using bank cards or digital financial services.

During 2021 in Spain, for instance, the probably Turkish 'Fajar Ganz', 'Rayzky' or 'Aslan Neferler Tim', were engaging in SEO poisoning and participated in militant defacement of websites in the context of #OpIsrael; or the probably Ibero-American 'Crystal_MSF', disseminated SEO poisoning content and participated in militant defacement for #OpColombia.[7]

Continuing the trend of previous years, 81% of hacktivist attacks in 2021 were correlated with the presence of vulnerable and/or outdated software on the websites attacked. 8 out of 10 websites victimised by defacement in 2021 had some kind of software security flaw, which continues to be the number one risk factor for hacktivist victimisation.

In almost all of these websites defaced in 2021, the attackers did not inject ideologically charged content, but merely their aliases or self-referential mentions, as if they were signing graffiti in an act of vandalism, in this case cyber vandalism.

Of this total percentage, in 58% of the victimised websites, the vulnerability detected in the software was related to commercial content management systems, with WordPress being the most represented with 47%, followed by DotNetNuke or SharePoint (Microsoft environment) with 26%. The Microsoft software environment (IIS for the server, Windows as operating system, ASP.net as operating code, and DotNetNuke or SharePoint as content managers), which in 2021 ranked second in the percentage scale with 26%, rises by the same amount.

In line with this opportunity and vandalism-oriented hacktivism, the correlation between the vandalistic defacement of websites and preparatory tactics in the sequence of organised cyberthreat activity can already be considered a trend pattern in Spain. In 2021, this volume was consolidated at over 28%.[8]

One of the incidents that most prototypically exemplified during 2021 the drift of 'double-duty' hacktivism alongside preparatory tactics for organised cyberthreats was carried out by 'Moroccan Revolution', a collective identity acting under various individual aliases ('Neige_Ma', 'MoroccanHack Team' or 'moroccohack_team', among others) at least since 2016. It conducted defacement attacks in several countries. On 22 May 2021, the group defaced six private websites equipped with outdated ASP.net software, injecting them with a type of content that could be considered typically hacktivist due to its vindictive tone, namely the message in English "free Morocco" alongside images of immigration on the Spanish coast of Ceuta; at the same time, it took advantage of the defacements to monetise them by inserting SEO poisoning content in Japanese into some of the victimised websites.

Another typical example of intersection between vandalism hacktivism and cyberthreats spreading malicious code or malware, which occurred in Spain in 2021, is that of 'Mr.QLQ', an identity that has been operating since at least 2015, injecting into its defacements content alluding to the <<defence of Muslims in the world>> and, more specifically, against the war in Yemen. On 7 June, 2021, 'Mr.QLQ' damaged a private website20 developed with outdated WordPress software with general vindictive content, on which it also injected the webshell 'Mini Mani Mo Shell', which is commonly used in the field of cyberthreats as a backdoor to prepare a website for the insertion of malicious code with different functions, generally monetisable.[9]

Another typical example of intersection between vandalism hacktivism and cyberthreats spreading malicious code or malware, which occurred in Spain in 2021, is that of 'Mr.QLQ', an identity that has been operating since at least 2015, injecting into its defacements content alluding to the <<defence of Muslims in the world>> and, more specifically, against the war in Yemen. On 7 June, 2021, 'Mr.QLQ' damaged a private website20 developed with outdated WordPress software with general vindictive content, on which it also injected the webshell 'Mini Mani Mo Shell', which is commonly used in the field of cyberthreats as a backdoor to prepare a website for the insertion of malicious code with different functions, generally monetisable.

In general, the websites of public administrations victimised during 2021 in Spain fall into one of three categories:

1. **Websites of universities and secondary education centres**, dependent on the government of Autonomous Communities, which expose outdated software, generally Joomla or WordPress but also for Apache server management. This first category includes defacements on websites of the universities of Barcelona, Zaragoza, Lleida, Salamanca, or the Polytechnic or Complutense of Madrid, among others, generally subdomains of a department or teaching unit hosted in specific areas of the universities' websites. Also noteworthy is the compromise of websites programmed with outdated Joomla software from secondary education centres attached to the Regional Government of Extremadura.

2. **Websites with outdated versions of the Open Journal Systems content manager**, which host digital journals of universities or other public institutions. It is worth mentioning that the worldwide compromise of digital journal websites developed with Open Journal Systems software is constant, at least by two identities that use Turkish content in their defacements: 'KingSkrupellos' and 'Mr.Kro0oz.305', at least the second of which uses its attacks to inject web poisoning content. This happened in December 2021, when the former defaced a subdomain dedicated to digital magazines and hosted on the website of the Ministry of Justice, as well as another on the website of the University of Malaga.

3. **Websites of town councils or local corporations with out-of-date software**, generally vulnerable. The practice of defacing local and regional government websites is general and systematic on a weekly basis. It is favoured by the fact that, especially in the case of local government websites, attackers find a considerable incidence of outdated software, which they take advantage of in many cases to inject SEO poisoning content or scripts redirecting traffic to malicious websites.

3. Statistics

3.1 Increase in the proportion of cybercrime in relation to other criminal offences over the years

Year	% Increase
2017	5.7
2018	7.5
2019	9.9
2020	16.3
2021	15.6

Figure 1: Increase in the proportion of cybercrime in relation to other criminal offences over the years[10]

3.2 Cyber-Incidents against private entities

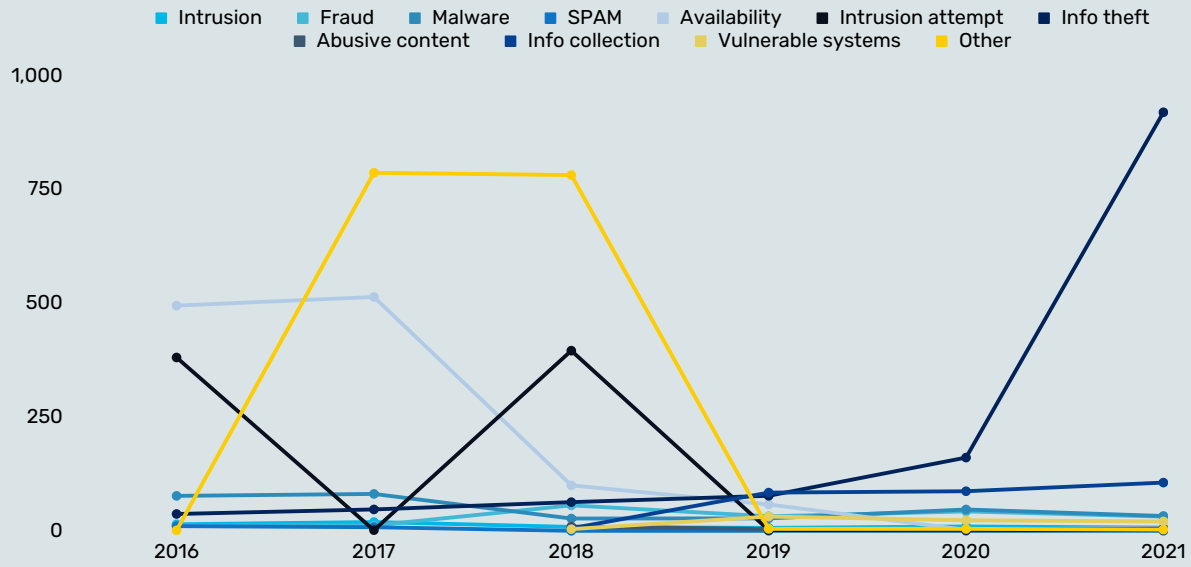

Figure 2: Cyber incidents against private entities[11]

3.3 Cyber-Incidents against critical infrastructure

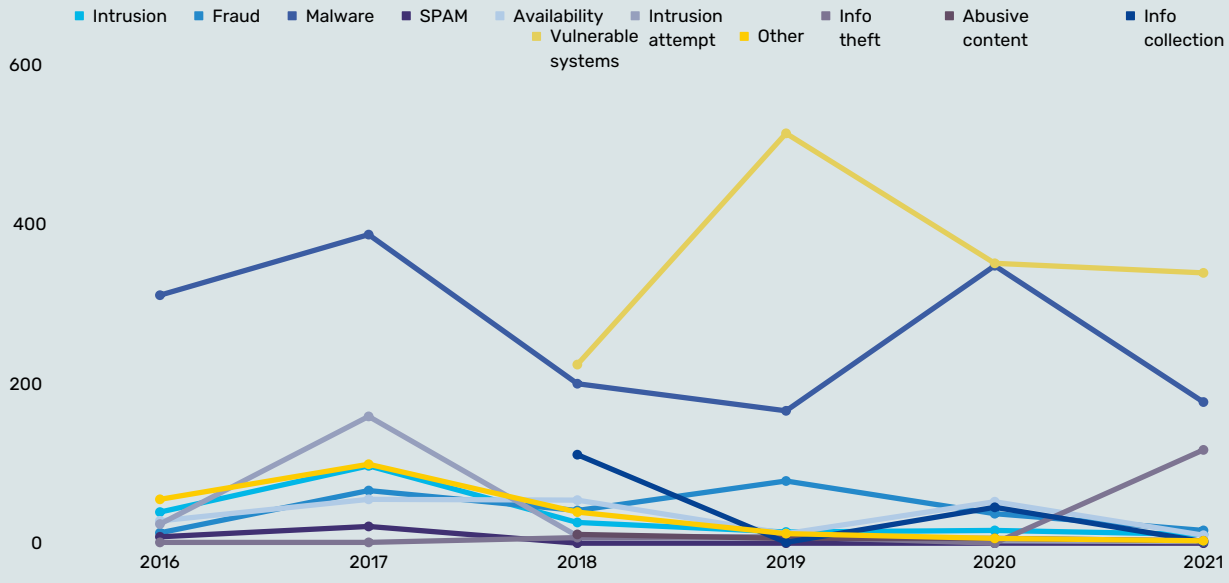

Figure 3: Cyber-Incidents against critical infrastructure[12]

3.4 Cyber-Incidents by strategic sector

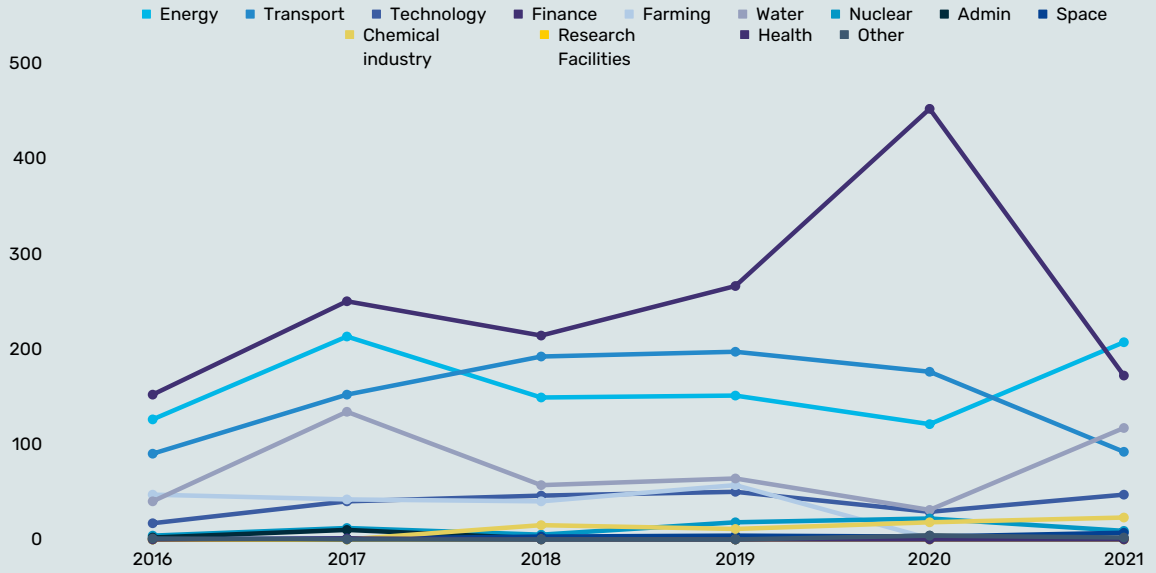

Figure 4: Cyber-Incidents by strategic sector [13]

3.5. Dissemination of cybercrime against private individuals

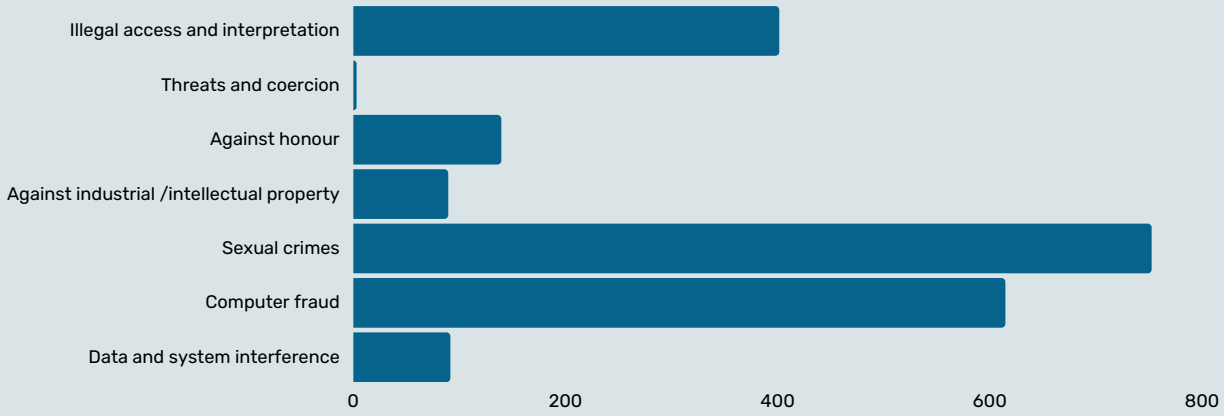

Figure 5: Dissemination of cybercrime against private individuals [14]

3.6 Recorded victimisations by type of crime and victims'age

Crime	Unknown	<18	18-25	26-40	41-50	51-65	>65
Illegal access and interpretation	3	350	944	1341	1039	748	130
Threats and coercion	42	1345	3111	6072	3907	255	554
Against Honour	20	89	201	470	394	244	43
Against industrial / intellectual property	1	0	2	14	26	17	2
Sexual crimes	10	1053	36	50	30	16	3
Computer forgery	14	212	1494	2561	1892	1590	412
Computer Fraud	179	668	26684	58587	50357	49949	18856
Data and system interference	0	16	132	449	594	483	109
Total Victimisation	269	3733	32604	69544	58239	55602	20109

Figure 6: Recorded victimisations by type of crime and victims' age[15]

4. Examples of counter measures

Within the Law Enforcement and Security Forces, intensive work was carried out in 2021 to combat cyber criminals. Two operations can be cited as examples:

4.1 Operation "SECRETO"

In this operation carried out by the National Police, an organisation was dismantled that had defrauded more than 12,000,000 EUR. As a result, 105 people were arrested and 14 others were charged in a macro-operation in which 88 simultaneous searches were carried out in four European countries.

The dismantled network created shell companies in the United States and, after providing them with a false economic solvency, requested the issuance of debit cards with the maximum amount available on the pretext of using them on their trips to Europe.

Once in Spain, the American debit cards were used in competing establishments for high amounts by means of the pre-authorisation system, taking advantage of the difference in payment acceptance between American and Spanish banks.

The investigation, which lasted for one and a half year, was led by the National Police together with the American Secret Service, with the participation of EUROPOL as well as the police forces of Greece, Austria, Denmark, United Kingdom, Germany, Poland and Ukraine.

The leaders of the group, of Albanian origin, used false Greek documents and had trusted personnel, all of them Spanish, who worked for the organisation in various functions. On the one hand, there were those who recruited conniving establishments, businessmen or self-employed people who allowed American cards to be swiped at their business' data-phone in exchange for a commission of 15% of the amount. Once the money was found in the connivant's account, the connivant would have to pay back the remaining 85% by bank transfer to one of the many accounts they managed.

The main members of the organisation both in Spain and in different European countries, in order to justify the supposed transaction, drew up false invoices in the name of the American companies that appeared on the card, with the aim of pretending to have bought products or provided a service.[16]

4.2 Operation "RECOLECTOR"

This operation by the Guardia Civil led to the dismantling of an international criminal organisation dedicated to committing crimes related to computer fraud in all its forms, with the arrest and investigation of eleven people in Spain and Chile.

The main activity of the network of cybercriminals was the illicit obtaining of data related to payment credentials (generally credit cards), both for direct exploitation on online trading platforms by the organisation itself, and for sale on channels of a well-known messaging app and on DarkWeb forums. This set of criminal activities is known in the world of cybercrime as CARDING.

The modus operandi identified was based, fundamentally, on the impersonation of real websites, a method known as phishing, belonging to national and international banking institutions, as well as well-known streaming multimedia content service companies, and thereby obtaining the victims' data.

In order to achieve their criminal objectives, they used different types of malwares such as the banking Trojan Zeus and TinyBanker, keyloggers, tools for denial-of-service attacks, bots, botnets and various types of ransomwares at their disposal.

The organisation was charged with more than 2,500 criminal acts with more than 300 companies affected nationwide, with an estimated damage to assets of up to one million EUR, and information was obtained on the use of more than 42,000 credit cards by the different members of the criminal organisation. Credit cards used by cybercriminals from 47 countries around the world have been located, especially those from the USA and European Union countries. [17]

References

1. This Policy Brief was prepared by the Guardia Civil of Spain, as part of T10.5.
2. Cf. National Cryptology Centre of Spain (CCN) (2021a), Cybercrime in 2021, Dec. 2021, at: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html.
3. Cf. CCN (2021a), Cybercrime in 2021. Cf. Cybercrime Statistical System of Spain (SEC) (2021), Cybercime Report, at: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/dam/jcr:fed95549-7365-485c-8cbe-15c84234cd86/Informe%20Cibercriminalidad%202021.pdf.
4. Cf. Europapress (2021) Europapress diary, 30 November 2021, at: https://www.europapress.es/portaltic/ciberseguridad/noticia-ciberataques-mas-importantes-2021-espana-sepe-phone-house-mediamarkt-20211130090050.html?utm_campaign=smartclip_social&utm_medium=Social&utm_source=Twitter.
5. Cf. CCN (2021b), Hacktivism in 2021. Annual Report, Dec. 2021, at: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6597-ccn-cert-ia-03-22-informe-anual-2021-hacktivismo-y-ciberyihadismo-paginas-enfrentadas-1/file.html.
6. Cf. CCN (2021b), Hacktivism in 2021. Annual Report.
7. Cf. CCN (2021b), Hacktivism in 2021. Annual Report.
8. Cf. CCN (2021b), Hacktivism in 2021. Annual Report.
9. Cf. CCN (2021b), Hacktivism in 2021. Annual Report.
10. Cf. SEC (2021), Cybercime Report.
11. Cf. SEC (2021), Cybercime Report.
12. Cf. SEC (2021), Cybercime Report.
13. Cf. SEC (2021), Cybercime Report.
14. Cf. SEC (2021), Cybercime Report.
15. Cf. SEC (2021), Cybercime Report.
16. Cf. SEC (2021), Cybercime Report.
17. Cf. SEC (2021), Cybercime Report.